AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

Information Associated with Steven Stenger cellular phone number [redacted] that is stored at premises owned, maintained, controlled, or operated by Apple, Inc.

Case No. 4:18 MJ 232 DDN

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the NORTHERN District of CALIFORNIA
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before August 20, 2018 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge David D. Noce
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____

Date and time issued: 10:51 am Aug. 6, 2018

David D. Noce
Judge's signature

City and state: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **Steven Stenger** cellular phone number [redacted] that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email

was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of inter alia, 18 U.S.C. § 666, 1341, 1343, and 1346 involving Steven Stenger since October 28, 2015, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and

f. Any and all records related to the directing of contracts and grants by Steven Stenger as well as his attempts to conceal these after the fact.

Any and all records that may constitute evidence of crimes, wrongs, or other acts that may be admissible to prove motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident, or that may be admissible for any other purpose pursuant to Fed. R. Evid. 404(b).

AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

FILED
AUG -6 2018
U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

for the
Eastern District of Missouri

In the Matter of the Search of

Information Associated with Steven Stenger cellular phone number [redacted] that is stored at premises owned, maintained, controlled, or operated by Apple, Inc.

Case No. 4:18 MJ 232 DDN

APPLICATION FOR A SEARCH WARRANT

I, Andrew R. Ryder, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 666	Theft or bribery concerning programs receiving Federal funds
18 U.S.C. Section 1346	Honest Services Fraud
18 U.S.C. Sections 1341 and 1343	Mail and Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrew R. Ryder
Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: Aug. 6, 2018

Judge's signature

City and state: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge
Printed name and title

AUSA: Hal Goldsmith

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

In the Matter of the Search of Information Associated with **Steven Stenger** and cellular phone number [redacted] **that is stored at premises controlled by Apple, Inc.**	Case No. 4:18 MJ 232 DDN **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Andrew R. Ryder, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with **Steven Stenger** and cellular phone number [redacted] (hereafter "Account") that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed since 2002. I am presently assigned to the Public Corruption squad in the St. Louis Division of the FBI. My responsibilities include the investigation of federal crimes to include violations of Title 18 United States Code (U.S.C.) § 666 (Theft or bribery concerning programs receiving Federal funds), § 1346 (Honest Services Fruad), § 1341 (Frauds and swindles) and § 1343 (Wire Fraud). I am currently assigned to investigate allegations of public corruption. I received over eighteen weeks of specialized law enforcement training at the FBI Academy in Quantico, Virginia. My experience obtained as a Special Agent of the FBI has included

investigations of multiple violations of federal criminal public corruption laws. I know cellular telephones are commonly used by politicians to communicate with donors, constituents, and employees. Cellular telephones enable a politician to communicate during the day when they are not at an office location, which is common with this type of work. Cellular telephones also enable the user to quickly send text messages to other people when they are unable to take the time to make a phone call, but the sender needs to quickly convey their message.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. Section 666 (Theft or bribery concerning programs receiving Federal funds), 18 U.S.C. Section 1346 (Honest Services Fraud), or 18 U.S.C. Sections 1341 and 1343 (Mail and Wire Fraud) have been committed by Steven Stenger, St. Louis County Executive. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

1. On March 5, 2018, the FBI opened an investigation based on an allegation the Executive Director of the St. Louis County Port Authority, Sheila Sweeney, used Port Authority funds to pay Cardinal Creative Consulting $130,000 for a marketing contract. The original allegation indicated the contract was payback for political donations made to St. Louis County Executive Steve Stenger, and little or no work was actually performed. Multiple sources of information, including individuals named below, have described to myself and others at the FBI a pattern whereby St. Louis County Executive Steve Stenger directs contracts and grants to be awarded to individuals and companies who have contributed to Stenger's re-election campaign. When Stenger became at odds with the majority of members of the St. Louis County Council, and lost the ability to utilize the St. Louis County Council to reward his donors, he recognized the opportunity to use money from the St. Louis County Port Authority for this purpose. The St. Louis

County Port Authority has an annual operating budget of approximately $4.0 million. Shortly after Sweeney was hired as Executive Director in September 2015, Stenger began directing the actions of the Port Authority relative to its grants and contracts. In addition to the Cardinal Creative contract, multiple other contracts and grants were directed by Stenger, using Sweeney and the SLCPA, for donors to Stenger's re-election campaign.

2. [redacted]

a. Rallo [redacted] met St. Louis County Executive Steve Stenger in or around August 2014 at Sam's Steakhouse. Rallo's friend Sorkis Webbe set up the meeting. Rallo met with Stenger with the hope of securing a benefit in exchange for a campaign donation. Rallo told Stenger he wanted a "fair shot" at obtaining the county's employee insurance contract through his company Cardinal Insurance. Rallo said he committed to giving Stenger $5,000 for this promise. Stenger told him he could make the contract a reality as those involved with the approval process "are under me." Rallo told Stenger that he was tired of giving money to politicians and not getting anything in return. Stenger told him, "That won't happen with me." Rallo [redacted] wrote two campaign donation checks that evening totaling $5,000, and handed them to Stenger at the dinner table. Rallo made significant additional campaign donations to Stenger following that initial meeting, all with the understanding that Stenger would assist Rallo in obtaining one or more contracts in St. Louis County.

b. The subsequent 2015 SLCPA consulting contract for CCC was a "payback contract" for Rallo's insurance company not having received the St. Louis County voluntary benefits insurance contract which St. Louis County Executive Steve Stenger had promised to Rallo in exchange for his campaign donations.

c. At Stenger's direction, beginning on or about October 2015, SLCPA Executive Director Sheila Sweeney met with Rallo on multiple occasions to discuss the CCC contract amount. Stenger told Rallo that Sweeney has the money in her budget,

and she does not have to go through the County Council to get approval. Rallo proposed $240,000 to Sweeney, but it was agreed upon at $100,000.

d. During their discussions, Sweeney revealed to Rallo that she had been told by Stenger that [redacted] helped get Stenger the North County vote and Stenger needed to get money to [redacted] John Cross. Shortly after the CCC contract was awarded at $100,000, Sweeney told Rallo she was adding $30,000 to the consulting contract because Steve Stenger had directed her to pay that amount to John Cross. Sweeney told Rallo to pay $30,000 to John Cross. Cross did not do any work on the CCC contract with the SLCPA, and Rallo paid him $25,000 from his proceeds under the contract. During that time, [redacted] Sweeney saying to Rallo, "What did I get myself into" in regard to having to "take care of Stenger's people".

e. In December 2017 there were a series of text messages between Rallo and Sweeney related to negative newspaper articles about Cardinal Creative and the SLPCA consulting contract. [redacted] Sweeney told him to get his name off of all of his LLC's and have the attorney's name on them instead. [redacted] Sweeney was referring to Rallo's name appearing as the Registered Agent on the Missouri Secretary of State website when his LLC's are searched. [redacted] Sweeney did not want people to be able to see Rallo was associated with companies that were awarded contracts through the SLCPA. [redacted] Sweeney's text message to him that, "Got to cover him! And me too!!!!" refers to covering Steve Stenger and

herself, [redacted] he found a lawyer and removed his name as Registered Agent for Cardinal Creative Consulting as Sweeney had instructed.

f. [redacted] he had no consulting experience, his bid was "complete bullshit", and this contract was 100% due to his campaign political contributions made to Stenger.

g. [redacted] he primarily texted with Stenger and he did not correspond with him via e-mail. [redacted] one of the phones carried by Stenger was an Apple device.

3. An FBI forensic review of Rallo's cellular phone identified a series of text messages between Rallo and Stenger [redacted]

a. On October 28, 2015, Rallo sent Stenger a text message, "Spoke w/Sheila (Sweeney) re: Montel…sounds like things are not going to move forward. Diametrically different from our conversation in your office. Let me know when you have a min to talk." Stenger, using cellular telephone [redacted], replied by text, "The 350k won't work for their budget but some other amount would. Needs to be negotiated." The FBI assesses there were different amounts discussed during the negotiations between Stenger/Sweeney/Rallo, accounting for the difference between $240,000 (above) and $350,000 in this text from Stenger. The final amount of the contract was $100,000.

b. On January 13, 2016, Stenger, using cellular telephone [redacted], sent a text to Rallo, "Have you made contact with Sheila at the partnership since we spoke?" Rallo responded, "I have not, I was going to send you a one page bullet pt outline as we discussed. Should I reach out to her again directly?" Stenger replied by text, "Shoot me the one pager when u can. I am meeting with Jeff now talking about things we need to take care of soon and this was on my agenda."

c. During a text message exchange starting on March 28, 2016, Stenger asked Rallo for campaign money (Citizens for Steve Stenger) to come in before the end of the quarter, "John, is there a way we would be able to get your 2500 for the quarter dated 3.31 in the next few days so we could count it for this quarter. We are trying

to hit 300k for the quarter and it would be helpful." After the two arrange for pick up of the check, on March 31, 2016 Rallo replies, "Check is ready! Need 5 min call to go over a concern I have on the insurance RFP…are u avail later today?"

4. [redacted]

a. In September 2015, Sweeney became the Executive Director of the SLCPA. She quickly learned that any contracts and grants had to be approved, and were usually directed, by Stenger. Stenger views use of the Port Authority's funds as the perfect way to avoid having to seek approval through the County Council for St. Louis County contracts. If Sweeney does not consult with Stenger before making a decision, the "wrath" of Stenger will come down upon her. [redacted] there were very few contracts or grants at the Port Authority that Stenger didn't personally direct to be made. In many of these instances Stenger told Sweeney the contract/grant was for a campaign donor.

b. In a meeting in Stenger's office, Stenger told Sweeney that John Rallo was Stenger's "friend" and that Stenger really wanted Rallo's Cardinal Creative Consulting to get a consulting contract from the SLCPA. Stenger told Sweeney to make it a $100,000 contract. Sweeney helped get CCC's bid selected by the Port Authority board, although there were more qualified bids. [redacted] it was not a fair bidding process, and she was directed by Stenger to give it to Rallo because of his donor relationship.

c. Later, in Stenger's office, Stenger told Sweeney he needed to get $30,000 to John Cross, [redacted] "guy". Stenger followed up with Sweeney several times, asking if she had figured out a way to get Cross the money. Sweeney decided the best way to get Cross the money was to add him to the CCC contract. There was no expectation Cross was going to do actual work for the money. Sweeney did not tell

the SLCPA board that Stenger told Sweeney to select CCC. Sweeney did not tell the SLCPA board that Stenger told her to get $30,000 to Cross.

d. When the media (St. Louis Post-Dispatch) began asking questions about the CCC contract, Stenger sent his media people to Sweeney to reiterate what to say. CCC's hiring of Montel Williams was the important message emphasized to Sweeney. Sweeney followed that direction even though she knew it was not true.

5. On June 23, 2018, the St. Louis Post-Dispatch printed an article titled "Documents raise questions about St. Louis Economic Development Partnership bidding procedures", by Jacob Barker. The article detailed the communications between John Rallo and Sheila Sweeney. Based on text messages reviewed by the FBI, it appears the newspaper reached out to various people, including Stenger and Sweeney in the days leading up to the article, attempting to get comments from them.

a. In a June 16, 2018 text message from Stenger's telephone, [redacted], Stenger wrote to Sweeney, "Please don't talk to him (Barker) till we talk and let's review his questions together." Sweeney responded one minute later, "Will do. And i don't plan to talk to him. But once i have the questions I'll let you know. Nothing good can come of talking to him."

b. In a group text message on June 23, 2018 after the online article release but before the print article, Stenger was one of several individuals exchanging text messages in a group text thread. In response to the article being a campaign piece for Stenger's opponent, Stenger texted, "Yeah. It's basically defamatory." St. Louis Economic Development Partnership Vice President of Marketing and Communications, Katy Jamboretz, in the text communications thread, wrote, "It would substantially help our case if we can send him the Sheila/Steve Grelle email that says don't treat John Rallo any different than any other person." [redacted] this information from the text message to not treat Rallo differently was based on a different deal than the Cardinal Creative deal. On the Cardinal Creative deal, which is what the newspaper was asking about at

the time, Rallo was treated differently because he was a donor and Stenger instructed Sweeney to get Rallo the contract.

6. A forensic review of Sweeney's cellular phone identified a text thread between Sweeney, Stenger, and Stenger's then chief of staff, Jeff Wagener. On November 10, 2015, Sweeney sent the text, "How much do you want approved for the Spanish Lake development corporation for salaries? Port meeting is today." Stenger replied on November 10, 2015 with a text message from telephone [redacted], "Let's look at it what did they ask for". Sweeney responded two minutes later, "This is just the amount to cover Jo R." (an individual hired by Sweeney at Stenger's direction). Sweeney then texted, "Mike O'Mara told me you had a number in mind. Like 25 or 30k." Stenger replied by text, "30". The SLCPA records show the board approved a $30,000 grant on that same date to the Spanish Lake Community Association. This text message is an example of Stenger using text messaging to direct the actions of the Port Authority.

7. There have been allegations of Stenger requiring campaign contributions before signing contracts or directing SLCPA contracts to large donors.

a. St. Louis Post-Dispatch printed an article dated March 13, 2017 titled "Meet the low-profile group that wields big power in St. Louis County". The article describes how the St. Louis County Port Authority's actions "don't ultimately go back to a legislative body – in this case, the St. Louis County Council – for final approval. It doles out millions of dollars a year in grants and contracts, one of which was awarded without other bids, possibly in violation of state statute." The article then discussed a $50,000 contract with Clayton-based Blitz, Bardgett and Deutsch for legal services related to a project. In December the SLCPA increased the amount to $75,000. Bob Blitz, according to the article, wrote a $12,500 check in January 2017 and made an $8,000 donation in 2016 to Stenger's campaign account. The article wrote "Stenger said he had no role in the contracts and noted that the port authority board members were all appointed by former county executives. 'I played no role – directly or indirectly – in the port authority board's decision to hire Blitz, Bardgett, & Deutsch to handle these legal matters. I have no supervisory authority over the port authority, its board, its management or individuals hired by it.'" [redacted]

[redacted] these public statements were false. [redacted]

b. A text thread was reviewed as part of a forensic examination of Sheila Sweeney's cellular phone. Several people were on the thread, including Sweeney and Stenger. The substance of the texts is deciding how to respond to a newspaper request for information regarding the hiring of Bob Blitz. On March 9, 2017, Stenger, using telephone [redacted] sent the text, "I think this would be my response," followed by, "I played no role directly or indirectly in the decision to hire Attorney Bob Blitz or his firm in these matters. I have no supervisory authority over the organization(s) or the individuals mentioned." Other individuals offered suggestions about how to respond.

c. [redacted] this statement by Stenger was not true. [redacted]

8. Stenger told Sweeney that John Rallo was a member of the "10,000 Club", who were individual donors who had committed to giving Stenger $10,000 or more annually. During mid to late 2016, Stenger told Sweeney Rallo wanted to develop property owned by the St. Louis County Land Clearance for Redevelopment Authority in Wellston, and Stenger wanted Rallo to get the contract. At Stenger's direction, Sweeney helped Rallo with the bidding process for the two separate pieces of land by reviewing his proposed bids and offering suggested revisions, including how much he should bid. Sweeney gave Rallo her personal email address to communicate with her so other people would not know she was reviewing Rallo's bid. Rallo's company, Wellston Holdings, LLC was the highest bidder on one contract, which he won. Sweeney did not tell the Port Authority board that Stenger directed Sweeney to give Rallo the contracts.

9. [redacted]

[redacted]

10. The FBI has debriefed numerous [redacted] people with knowledge of the individuals discussed throughout this affidavit, as well as Steve Stenger's conduct in these matters. These individuals include current and former members of St. Louis County government. Their accounts of the "pay to play" politics under St. Louis County Executive Steve Stenger are consistent with the information included herein.

11. Based on my training and experience, I know that text messages sent between Steve Stenger and others were sent and received on Apple devices given the way that they appeared on Sheila Sweeney's and John Rallo's phones during forensic reviews of their phones.

12. A preservation request was sent to Apple, Inc. for **Steven Stenger** and cellular phone number [redacted] on July 30, 2018.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

1. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

2. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased

through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

3. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

4. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

5. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

6. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records

relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

7. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

8. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

9. The United States is investigating allegations that St. Louis County Executive Steven Stenger is directing and approving St. Louis County contracts and grants to individuals and companies only after contributions are made to his re-election campaign, and is utilizing St. Louis

County Port Authority funds to reward large donors to his re-election campaign. The allegations disclose possible violations of 18 U.S.C. Sections 666, 1341, 1343, and 1346. In my training and experience, evidence of who was using an Apple ID, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

10. As stated above, Steve Stenger sent iMessages related to the awarding of contracts and his efforts to conceal those acts. Stored communications and files from the account that is the subject of this affidavit are vital to this ongoing investigation. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, including with this investigation, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

11. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

12. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

13. As stated above, the investigation to date has revealed that Steven Stenger sent iMessages to Sheila Sweeney, John Rallo, and others related to the awarding of contracts to political donors and the attempt to conceal these awards after the fact. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

14. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

1. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple, Inc. to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

1. Based on the forgoing, I request that the Court issue the proposed search warrant.

2. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

3. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

4. The foregoing has been reviewed by Hal Goldsmith, Assistant United States Attorney, U.S. Attorney's Office, Eastern District of Missouri.

REQUEST FOR SEALING

1. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Further, it discloses the identities of government witnesses who might fact retribution if their identities are disclosed. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation or cause harm to government witnesses.

Respectfully submitted,

Andrew R. Ryder, Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN BEFORE ME THIS 6th DAY OF AUGUST, 2018.

HONORABLE DAVID D. NOCE
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **Steven Stenger** cellular phone number [redacted] that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email

was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of inter alia, 18 U.S.C. §§666, 1341, 1343, and 1346 involving Steven Stenger since October 28, 2015, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and

f. Any and all records related to the directing of contracts and grants by Steven Stenger as well as his attempts to conceal these after the fact.

Any and all records that may constitute evidence of crimes, wrongs, or other acts that may be admissible to prove motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident, or that may be admissible for any other purpose pursuant to Fed. R. Evid. 404(b).